BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C. 20554

In the Matter of	)	
	)	
Call Authentication Trust Anchor	)	WC Docket No. 17-97
	)	

COMMENTS OF THE EDISON ELECTRIC INSTITUTE TO NOTICE OF INQUIRY

Edison Electric Institute

Phillip Moeller
Executive Vice President,
Business Operations Group and
Regulatory Affairs

Aryeh B. Fishman
Associate General Counsel,
Regulatory Legal Affairs
Office of the General Counsel

EDISON ELECTRIC INSTITUTE
701 Pennsylvania Avenue, NW
Washington, DC 20004-2696
(202) 508-5000

August 14, 2017

Pursuant to sections 1.415 and 1.419 of the Federal Communications Commission's ("FCC" or "Commission") Rules, the Edison Electric Institute ("EEI"), on behalf of its member companies, hereby submits these Comments in response to the above-referenced Notice of Inquiry ("NOI")[1] to support the Commission's effort to better protect American consumers from fraudulent wireless and wireline calls by facilitating methods to authenticate telephone calls which may help deter illegal robocalls and other callers.

EEI is the trade association that represents all U.S. investor-owned electric companies. Our members provide electricity for 220 million Americans, and operate in all 50 states and the District of Columbia. As a whole, the electric power industry supports more than 7 million jobs in communities across the United States. In addition to our U.S. members, EEI has more than 60 international electric companies, with operations in more than 90 countries, as International Members, and hundreds of industry suppliers and related organizations as Associate Members. Organized in 1933, EEI provides public policy leadership, strategic business intelligence, and essential conferences and forums.

EEI's members are major users of telecommunications systems to support the goals of clean power, grid modernization, and promoting customer solutions. As owners and operators of a significant portion of the U.S. electricity grid, EEI has filed comments before the Commission in various proceedings affecting the telecommunications' interests of its members who are impacted by the FCC's rules and policies. Accordingly, EEI and its members have a strong interest in the Commission's proposals to protect American consumers, including utility customers, from unwanted and illegal robocalls and other calls.

[1] *See In the Matter of Call Authentication Trust Anchor*, Notice of Inquiry, WC Docket No. 17-97 (adopted July 13, 2017).

I. Introduction

In this proceding, the Commission explores how it can further protect the nation's telephone networks and consumers against unwanted and often fraudulent robocalls by facilitating use of methods to authenticate telephone calls and thus deter illegal robocalls.[2] The NOI correctly acknowledges criminals are using accessible technologies to spoof their call identity and scam victims with certain threats.[3] Across North America, the utility industry has experienced scams involving criminals spoofing utility telephone numbers, posing as utility employees, calling utility customers, threatening disconnection of service and demanding payment by prepaid, credit, or gift cards.

In this regard, North American utility customers are reporting millions of dollars lost annually to scams. In a recent report published by the Better Business Bureau ("BBB"), it found that more than 32,000 reports were submitted to its Scam Tracker, with an average of about one report received every 15 minutes, with the top means of consumer contact by scammers (over 20 percent) being telephonic and the median financial loss to consumers being $274.[4] Of the 30 different types of scams tracked and categorized by BBB, utility scams victims were found to have a median financial loss of $500 with the top payment method being prepaid cards.[5]

---

[2] *See* NOI at P 1.
[3] *See* NOI at P 2.
[4] *See* Emma Fletcher and Rubens Pessanha, *2016 BBB Scam Tracker Annual Risk Report: A New Paradigm for Understanding Scam Risk* (Feb. 25, 2017) (2016 BBB Report) at pages 6 and 14; see https://www.bbb.org/globalassets/local-bbbs/council-113/media/scam-tracker/risk-report/bbbscamtrackerannualreport-022517-v3.pdf.
[5] *See* 2016 BBB Report at P 21.

Through consumer reports, BBB has found that people are more susceptible to utility scams than they are to Internal Revenue Service scams.[6]

As mentioned, criminals frequently utilize caller identification ("ID") spoofing to pose as utility company representatives, falsely claim to be calling about a past due utility bill, and demand immediate payment via prepaid cards or other means to avoid same-day utility service disconnection.[7] Though it does not appear these scammers are employing robocalling on a widespread basis (yet),[8] they are employing sophisticated spoofing tactics, to display a utility company's name on the customer's caller ID and to disguise their identity and criminal intentions, and recordings of utility company telephone menu messages, or interactive voice response systems, resulting in significant customer financial losses. Frequently, these criminals are targeting vulnerable populations, including senior citizens and non-native English speakers. The NOI correctly asserts that these calls harm more than their recipients because not only is the customer harmed, but the business' reputation is potentially marred in its local area.[9] In fact, some of EEI's member utilities have had to defend lawsuits filed against them by customers who have lost money to utility scams, and have had to defend lawsuits brought under the Telephone

---

[6] *See* 2016 BBB Report at P 21. According to the BBB report, the susceptibility rate for tax collection scams is 0.9 percent while the susceptibility rate for utility scams is 6.6%. The NOI describes criminals using technologies to spoof their caller identity and scam victims with false threats of legal action from the Internal Revenue Service. *See* NOI at P 4. BBB Scam Tracker, a free interactive online tool (bbb.org/scamtracker), was launched by BBB in November 2015 to provide consumers across North America with a place to report scams and fraud, and to warn others of malicious or suspicious activities. All 112 BBBs operating in Canada and the U.S. are now collecting information from consumers and processing data, which is shared with law enforcement agencies for use in identifying and prosecuting scammers. *See* https://www.bbb.org/news-release-bbb-scam-tracker/.

[7] *See, e.g., SCE SCAM*, https://www.youtube.com/watch?v=dvjkG1K-2uk (this is a recording posted on YouTube of a scammer that spoofed Southern California Edison's ("SCE") phone number, pretended to be SCE on the phone with SCE's customer, tried to defraud the customer of money by threatening disconnection, and left a different call back number for the customer to call back with a prepaid card. In this scam, the the spoofer's call center mimics SCE's Interactive Voice Response systems ("IVRs").

[8] EEI understands some electric customers get robocalls alleging to be from a utility but it is not known whether these calls are also related to live-person calls spoofing utility telephone numbers.

[9] *See* NOI at P 2.

Consumer Protection and Caller ID Act based on calls made by third parties spoofing a utility phone numbers.

EEI would like to take this opportunity to provide comments to the FCC about its member utilities' work in collaborating with each other to educate consumers on scams, partnering with the telecommunications industry to learn more about its practices and share information to disconnect fraudulently-used telephone numbers, and engaging with technology companies to authenticate utility company telephone numbers, making consumers more aware of potential scammers.

II. Utilities United Against Scams

Given the serious impacts associated with utility scams and particularly the problems associated with scammers' fraudulent use of toll-free numbers, beginning in 2016, the utility industry, including electric, gas and water companies, began its efforts to organize a first-of-its-kind, all-utility collaborative, Utilities United Against Scams ("UUAS"). UUAS has grown to over one hundred utility members in the one year since the initiative began. EEI and other utility trade associations are members of UUAS.

This group's mission is to combat utility scams by providing a forum for utility companies and associations to share data and best practices and to work together to implement initiatives to inform and protect customers. UUAS not only works to educate customers about telephonic scam tactics but also has extended its collaboration beyond the utility industry to other interested and affected stakeholders. Beginning in early 2017, UUAS began meeting with USTelecom, which has educated UUAS members on SHAKEN/STIR, traceback, "do not originate," and its ongoing work with the FCC and Robocall Strike Force. Equally notable, in

2017, UUAS began working with Somos, which has operated, managed, and administered the SMS/800 Toll-Free Number ("TFN") Registry under the FCC tariff, enabling Toll-Free Service Providers to reserve and manage Toll-Free Numbers since 1993.[10]

III. Caller Identification Spoofing

Somos manages over forty million TFNs. Somos provides SMS/800 functions to Responsible Organizations ("Resp Orgs") through operation of the SMS/800, an operations and administrative support system used for the creation and maintenance of call processing records from TFNs and a source of TFN availability and reservation status information. The SMS/800 receives from the Resp Org the toll-free subscriber record and call routing information associated with the TFNs reserved by, or assigned to, the Resp Org. Resp Orgs are businesses that have undergone a certification process to obtain SMS/800 privileges, as designated by the Commission.

Somos is helping UUAS in stopping scams. Unknown to Resp Orgs, scammers use fake identification and fraudulent credit cards for payments relating to their request of multiple TFNs. The criminals then change the caller name identification associated with the number, but not the TFN, to a utility company name.

Under the FCC tariff, TFNs are prohibited from being used for "any unlawful purpose."[11] As the Toll-Free Neutral Administrator, Somos ensures the health and vibrancy of the Toll-Free ecosystem, and fighting fraud is part of that role. Therefore, Somos can contact its Resp Orgs,

---

[10] Tariff FCC No. 1, Somos, Inc., *800 Service Management Systems (SMS/800) Functions: Regulations, Rates and Charges Applying to the Provision of SMS/800 Functions and Support Services*, Issued under the authority of Order, *In re Toll Free Service Access Codes*, 28 FCC Rcd 15328 (2013), Issued Nov. 3, 2015 and effective Nov. 18, 2015; *see* https://s3.amazonaws.com/files-prod.somos.com/documents/SMS800FunctionsTariff.pdf.

[11] Tariff FCC No. 1, Section 2.2.2 at P 25.

which, among other things, investigate fraudulent use of TFNs and shutdown numbers used for scams.

UUAS members report to Somos the known TFNs that scammers are fraudulently using for calling utility customers and/or using to clone utility interactive voice response messages. Somos sends the reported TFNs to the Resp Org that reviews the complaint, confirms the misuse, and disconnects the number by pulling its routing ensuring the number is no longer in service. This process can take seconds or days. The Resp Org reports to Somos the conclusion of the investigation. Sometimes, patterns can be determined if a scammer picks up multiple TFNs from Resp Orgs and the Resp Org can then determine if a block of numbers is being utilized by criminals, shutting down those numbers immediately. UUAS has provided Somos with TFNs being used by scammers and Somos has been able to assist UUAS by helping shut down those numbers.[12]

To give the Commission as sense of the scale of the problem it is trying to address with this NOI, consider that SCE, an EEI member and electric utility that serves 180 incorporated cities, 15 counties, 50,000 square miles of service area in central and southern California, between January 1 and July 31, 2017, had customers receive 1,081 robocalls appearing to be from SCE's IVRs. These are calls that SCE did not make and in many cases these calls appeared to be from SCE IVRs that are not even capable of making outbound calls. SCE learned of these calls from complaints made to SCE by the call recipients, two-thirds of whom were SCE customers. Since January 1, 2017, SCE customers have received over 6,400 fraud calls,[13] with scammers demanding $2,478,905.96. Unfortunately, despite education efforts like those

[12] EEI understands that, to date, there have been over 200 TFNs shut down by Somos on behalf of UUAS members.
[13] This represents only those calls that SCE is aware of and SCE believes the actual numbers of calls, total money demanded and defrauded from customers to be much higher.

described through UUAS, SCE customers have paid $334,617.72 to these scammers, year to date.

Although the primary concern related to these scams is the injury to the customer, SCE also suffers reputational harm from these bad actors' behavior while impersonating the utility. Since June 9, 2017, SCE has disconnected 206 TFNs associated with these types of scams. SCE has sent over 190 TFNs to Somos[14] to shut down, as well as twelve TFNs to magicJack[15] and one TFN to Text plus.[16] In order to file a complaint, SCE needs to know the identity of the carrier. If a search does not provide a carrier, SCE has worked successfully with a company called Synverse that researches the carrier and enables SCE to make a complaint.

IV. Caller Authentication

Another way EEI member companies are helping their utility customers avoid becoming scam victims is through the consideration of caller identification technologies to authenticate utility company telephone numbers for their customers. When a utility calls their customer, either to a wireless or wireline telephone, these technologies may be able to identify the utility with a verified utility business logo, company website, security credentials for a verified number, or other identifying features rather than only the typical caller ID name, number, and location of the caller. Such technologies may also be able to flag certain calls or provide fraud alerts to the utility's customers. These types of partnerships between utilities and technology companies are still in the early stages.

[14] Somos learned that some of these TFNs had already been shut down.
[15] According to their own website, "magicJack owns one of the largest US Wireline-based Telecom company in terms of home phone numbers available and certifications." *See* http://www.vocaltec.com/.
[16] *See* https://textplus.com/about-us/.

VI. Conclusion

EEI applauds the work of UUAS, its member companies, and its partners, but recognizes there is a need for an even more comprehensive suite of tools to fight these types of scams. It is important for the Commission's effort in this proceeding to explore a range of possible solutions and the FCC's NOI is a promising step in the right direction. Malicious actors are hiding their true originating phone numbers, and putting investigators, enforcers, and consumers at a disadvantage.[17] Accordingly, EEI appreciates this opportunity to highlight the work its member utility companies are engaged in to combat scams and inform consumers.

Respectfully submitted,

EDISON ELECTRIC INSTITUTE

/s/ Phillip Moeller
Phillip Moeller
Executive Vice President,
Business Operations Group and Regulatory Affairs

Aryeh B. Fishman
Associate General Counsel, Regulatory Legal Affairs
Edison Electric Institute
Washington, D.C. 20004
(202) 508-5000
afishman@eei.org

Dated: August 14, 2017

[17] *See* NOI at P 3.